UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/531,173	04/11/2005	Kan Torii	00862.023417.	5079

5514 7590 06/16/2009

FITZPATRICK CELLA HARPER & SCINTO
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
06/16/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/531,173	TORII, KAN	
	Examiner	Art Unit	
	ELENI A. SHIFERAW	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03/27/2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-7 and 9-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-7 and 9-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1. Claims 1, 3-7, and 9-19 are pending in this Office Action.

All independent claims are amended.

Claims 2 and 8 are previously canceled.

2. Claims 1 and 16 have been fully considered for statutory reason and have been interpreted as statutory in light of applicant's disclosure page 9 line 7 wherein said "an input unit" is a key board and pointing device.

Response to Amendment and Arguments

3. The 112 rejection is withdrawn.

4. The 101 rejection is withdrawn in view of applicant's amendment.

5. Applicant's arguments filed on 12/24/2008 have been fully considered but are moot in view of new grounds of rejection.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 5, 6, 7, 11, 12, 13, 14, 16, 17, and 19 rejected under 35 U.S.C. 103(a) as being unpatentable over US 6021496 (Dutcher) (Applicant's IDS) in view of Chen et al. US PG Pubs. 20030028650 A1.

As to claim 1, Dutcher discloses an authentication apparatus having a plurality of authentication mechanisms, characterized by comprising: an input unit adapted to input authentication information of an object of authentication, said authentication information having been already authenticated by a first mechanism that is in use (Dutcher column 5, lines 5-8 and column 20, lines 6-49);

a determination unit adapted to determine whether the authentication information that has been input by said input unit corresponds to an object of authentication that has an authority to change over the first authentication mechanism in use to another authentication mechanism (Dutcher column 2, lines 55-64);

a display control unit adapted to display a list of the plurality of authentication mechanisms if it has been determined by said determination unit that the authentication information that has been input corresponds to the object of authentication that has the authority to make the changeover (Dutcher column 3, lines 8-15);

a registration unit adapted to register, as an effective authentication mechanism, ~~an~~ a second authentication mechanism that has been selected from the list displayed by said display control unit (Dutcher column 3, lines 16-23);

a verification unit adapted to verify that authentication of the object of authentication in the second authentication mechanism succeeds (Dutcher column 20, lines 6-49); and

an invalidation unit adapted to invalidate the first authentication mechanism, if it has been verified by the verification unit that the authentication of the object of authentication in the second authentication mechanism succeeds (Dutcher column 11, lines 26-49).

Dutcher fails to explicitly explain wherein changeover control step of controlling management of the object of authentication so that successful authentication of the object of authentication in the second authentication mechanism is verified before management is changed over from the first authentication mechanism to the second authentication mechanism, wherein the object of authentication continues to be in an authenticated state in the first authentication mechanism, and is not released from management under the first authentication mechanism, until successful authentication in the second authentication mechanism is verified.

However Chen et al. discloses a home office (101, 201, or 301 of fig. 1-3) and a corporate network (197, 297 or 397), a device in the home network connecting to a host device of the corporate network by connecting to the internet service provider ISP first by providing a user name and password (see fig. 7 and par. 0078). Once the user successfully logs-on (see par. 0079), a main menu (as shown in fig. 8) is displayed for the user to connect to another and authenticated (see fig. 14). The user is re authenticated but never lost the ISP connection upon new/other connection authentication (see fig. 3 and 6-14 and par. 0075-0095).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Chen et al. within the system of Dutcher because they are analogous in authentication and authorization for access. One would have been motivated to modify the teachings to provide the user the current service when the request for the second service is not valid.

As to claim 7, Dutcher discloses the authentication method of changing over a plurality of authentication mechanisms and performing authentication with any one of said plurality of authentication mechanisms, comprising:

an input step of inputting authentication information of an object of authentication, said authentication information having been already authenticated by a first authentication mechanism that is in use (Dutcher column 5, lines 5-8);

a determination step of determining whether the authentication information that has been input at said input step corresponds to an object of authentication that has an authority to change over the first authentication mechanism in use to another authentication mechanism (Dutcher column 2, lines 55-64);

a display control step of displaying a list of the plurality of authentication mechanisms if it has been determined at said determination step that the authentication information that has been input corresponds to the object of authentication that has the authority to make the changeover (Dutcher column 3, lines 8-15);

a registration step of registering, as an effective authentication mechanism, a second authentication mechanism that has been selected from the list displayed at said display control step (Dutcher column 3, lines 16-23);

a verification step of verifying that authentication of the object of authentication in the second authentication mechanism succeeds (Dutcher column 20, lines 6-49); and
an invalidation step of invalidating the first authentication mechanism, if it has been verified in the verification step that the authentication of the object of authentication in the second

authentication mechanism succeeds, wherein one or more of the foregoing steps is performed using a processor (Dutcher column 11, lines 26-49).

Dutcher fails to explicitly explain an invalidation changeover control step of controlling management of the object of authentication so that successful authentication of the object of authentication in the second authentication mechanism is verified before management is changed over from the first authentication mechanism to the second authentication mechanism, wherein the object of authentication continues to be in an authenticated state in the first authentication mechanism, and is not released from management under the first authentication mechanism, until successful authentication in the second authentication mechanism is verified.

However Chen et al. discloses a home office (101, 201, or 301 of fig. 1-3) and a corporate network (197, 297 or 397), a device in the home network connecting to a host device of the corporate network by connecting to the internet service provider ISP first by providing a user name and password (see fig. 7 and par. 0078). Once the user successfully logs-on (see par. 0079), a main menu (as shown in fig. 8) is displayed for the user to connect to another and authenticated (see fig. 14). The user is re authenticated but never lost the ISP connection upon new/other connection authentication (see fig. 3 and 6-14 and par. 0075-0095).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Chen et al. within the system of Dutcher because they are analogous in authentication and authorization for access. One would have been motivated to modify the teachings to provide the user the current service when the request for the second service is not valid.

As to claim 13, Dutcher discloses an authentication method comprising:

an input step of inputting authentication information of an object of authentication (Dutcher column 5, lines 5-8);

a first authentication step of authenticating whether an object of authentication has access right to a first system using the authentication information of the object of authentication that has been input at said input step, and allowing the object of authentication to access the first system if authentication succeeds (Dutcher Figure 4);

a second authentication step of authenticating whether the object of authentication has access right to a second system using the authentication information of the object of authentication that has been input at said input step, and allowing the object of authentication to access the second system if authentication succeeds (Dutcher column 5, lines 22-31);

a control step of controlling whether the object of authentication will be managed under management of the first system or under management of the second system (Dutcher column 6, lines 1-12); and

a verification step of verifying that authentication of the object of authentication in the second system has succeeded at said second authentication step; wherein if an instruction, that instructs to switch the object of authentication that is authenticated at the first authentication step from management under the first system to management under the second system, has been recognized, said control step controls said first authentication step and said second authentication step, in order to switch the object of authentication from management under the first system to management under the second system, on the condition that the authentication of the object of authentication at said second authentication step has been verified at said verification step,

wherein one or more of the foregoing steps is performed using a processor (Dutcher column 20, lines 6-49).

Dutcher fails to explicitly explain an invalidation changeover control step of controlling management of the object of authentication so that successful authentication of the object of authentication in the second authentication mechanism is verified before management is changed over from the first authentication mechanism to the second authentication mechanism, wherein the object of authentication continues to be in an authenticated state in the first authentication mechanism, and is not released from management under the first authentication mechanism, until successful authentication in the second authentication mechanism is verified, wherein one or more of the foregoing steps is performed using a processor.

However Chen et al. discloses a home office (101, 201, or 301 of fig. 1-3) and a corporate network (197, 297 or 397), a device in the home network connecting to a host device of the corporate network by connecting to the internet service provider ISP first by providing a user name and password (see fig. 7 and par. 0078). Once the user successfully logs-on (see par. 0079), a main menu (as shown in fig. 8) is displayed for the user to connect to another and authenticated (see fig. 14). The user is re authenticated but never lost the ISP connection upon new/other connection authentication (see fig. 3 and 6-14 and par. 0075-0095).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Chen et al. within the system of Dutcher because they are analogous in authentication and authorization for access. One would have been motivated to modify the teachings to provide the user the current service when the request for the second service is not valid.

As to claim 16, Dutcher discloses an authentication apparatus comprising:

an input unit adapted to input authentication information of an object of authentication (Dutcher column 5, lines 5-8);

a first authentication unit adapted to authenticate whether an object of authentication has access right to a first system using the authentication information of the object of authentication that has been input by said input unit, and allowing the object of authentication to access the first system if authentication succeeds (Dutcher Figure 4);

a second authentication unit adapted to authenticate whether the object of authentication has access right to a second system using the authentication information of the object of authentication that has been input by said input unit, and allowing the object of authentication to access the second system if authentication succeeds (Dutcher column 5, lines 22-31);

a control unit adapted to control whether the object of authentication will be managed under management of the first system or under management of the second system (Dutcher column 6, lines 1-12); and

a verification unit adapted to verify that authentication of the object of authentication in the second system by said second authentication unit has succeeded; wherein if an instruction, that instructs to switch the object of authentication that is authenticated at the first authentication step from management under the first system to management under the second system has been recognized, said control unit controls said first authentication unit and said second authentication unit, in order to switch the object of authentication from management under the first system to management under the second system, on the condition that the authentication of the object of

authentication by said second authentication unit has been verified by said verification unit (Dutcher column 20, lines 6-49).

Dutcher fails to explicitly explain an invalidation changeover control step of controlling management of the object of authentication so that successful authentication of the object of authentication in the second authentication mechanism is verified before management is changed over from the first authentication mechanism to the second authentication mechanism, wherein the object of authentication continues to be in an authenticated state in the first authentication mechanism, and is not released from management under the first authentication mechanism, until successful authentication in the second authentication mechanism is verified.

However Chen et al. discloses a home office (101, 201, or 301 of fig. 1-3) and a corporate network (197, 297 or 397), a device in the home network connecting to a host device of the corporate network by connecting to the internet service provider ISP first by providing a user name and password (see fig. 7 and par. 0078). Once the user successfully logs-on (see par. 0079), a main menu (as shown in fig. 8) is displayed for the user to connect to another and authenticated (see fig. 14). The user is re authenticated but never lost the ISP connection upon new/other connection authentication (see fig. 3 and 6-14 and par. 0075-0095).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Chen et al. within the system of Dutcher because they are analogous in authentication and authorization for access. One would have been motivated to modify the teachings to provide the user the current service when the request for the second service is not valid.

As to claim 19, Dutcher discloses an authentication program stored in a computer-readable storage medium comprising:

code for implementing an input step of inputting authentication information of an object of authentication (Dutcher column 5, lines 5-8);

code for implementing a first authentication step of authenticating whether an object of authentication has access right to a first system using the authentication information of the object of authentication that has been input at said input step, and allowing the object of authentication to access the first system if authentication succeeds (Dutcher Figure 4);

code for implementing a second authentication step of authenticating whether the object of authentication has access fight to a second system using the authentication information of the object of authentication that has been input at said input step, and allowing the object of authentication to access the second system if authentication succeeds (Dutcher column 5, lines 22-31);

code for implementing a control step of controlling whether the object of authentication will be managed under management of the first system or under management of the second system (Dutcher column 6, lines 1-12); and

code for implementing a verification step of verifying that authentication of the object of authentication in the second system has succeeded at said second authentication step; wherein if an instruction, that switches the object of authentication that is authenticated at the first authentication step from management under the first system to management under the second system~ has been recognized, said control step controls said first authentication step and said second authentication step, in order to switch the object of authentication from management

under the first system to management under the second system, on the condition that the authentication of the object of authentication at said second authentication step has been verified at said verification step (Dutcher column 20, lines 6-49).

Dutcher fails to explicitly explain an invalidation changeover control step of controlling management of the object of authentication so that successful authentication of the object of authentication in the second authentication mechanism is verified before management is changed over from the first authentication mechanism to the second authentication mechanism, wherein the object of authentication continues to be in an authenticated state in the first authentication mechanism, and is not released from management under the first authentication mechanism, until successful authentication in the second authentication mechanism is verified.

However Chen et al. discloses a home office (101, 201, or 301 of fig. 1-3) and a corporate network (197, 297 or 397), a device in the home network connecting to a host device of the corporate network by connecting to the internet service provider ISP first by providing a user name and password (see fig. 7 and par. 0078). Once the user successfully logs-on (see par. 0079), a main menu (as shown in fig. 8) is displayed for the user to connect to another and authenticated (see fig. 14). The user is re authenticated but never lost the ISP connection upon new/other connection authentication (see fig. 3 and 6-14 and par. 0075-0095).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Chen et al. within the system of Dutcher because they are analogous in authentication and authorization for access. One would have been motivated to modify the teachings to provide the user the current service when the request for the second service is not valid.

As to claim 5, Dutcher discloses the authentication apparatus according to claim 1, wherein each of said plurality of authentication mechanisms has: a storage unit that has registered authentication information of an object of authentication; and an authentication determination unit which, in a case where entered authentication information of a user has been registered in said storage unit, is for authenticating this object of authentication (Dutcher column 3, lines 16-19).

As to claim 6, Dutcher discloses the authentication apparatus according to claim 1, further having a start-up unit for starting up an authentication mechanism that has been registered as an effective authentication mechanism by said registration unit (Dutcher column 5, lines 8-21).

As to claim 11, Dutcher discloses ~~An~~ the authentication method according to claim 7, wherein each of said plurality of authentication mechanisms has a storage unit that registers authentication information of an object of authentication (Dutcher column 17, lines 67), and said method further has an authentication determination step which, in a case where entered authentication information of an object of authentication has been registered in said storage unit, is a step of authenticating this object of authentication (Dutcher column 3, lines 16-19).

As to claim 12, Dutcher discloses ~~An~~ the authentication method according to claim 7, further having a start-up step of starting up an authentication mechanism that has been registered as an effective authentication mechanism at said registration step (Dutcher column 5, lines 8-21).

As to claim 14, Dutcher discloses ~~An~~ the authentication method according to claim 13, wherein said control step controls said first authentication step in such a manner that the object

of authentication is excluded from management at said first authentication step in a case where it is verified at said verification step that the object of authentication has been authenticated at said second authentication step (Dutcher column 9, lines 20-26).

As to claim 17, Dutcher discloses ~~An~~ the authentication apparatus according to claim 16, wherein said control unit controls said first authentication unit in such a manner that the object of authentication is excluded from management by said first authentication unit in a case where it is verified by said verification unit that the object of authentication has been authenticated by said second authentication unit (Dutcher column 9, lines 20-26).

8. Claims 3, 4, 9, 10, 15, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 6021496 (Dutcher) (Applicant's IDS) and Chen et al. US PG Pubs. 20030028650 A1 as applied to claims 1, 7, 13, and 16 above, and in view of US 20020087894 (Foley) (Applicant's IDS).

As to claim 3, Currently Amended) Dutcher discloses ~~An~~ the authentication apparatus according to claim 1. Dutcher and Chen et al. fail to teach wherein said input unit reads a card on which authentication information of an object of authentication has been recorded and inputs said authentication information.

However, Foley discloses wherein said input unit reads a card on which authentication information of an object of authentication has been recorded and inputs said authentication information (Foley page 4, paragraph 0031).

It would be obvious to one of ordinary skill in the skill in the art at the time of the applicant's invention that smart cards were used to carry authentication information (Foley page 4, paragraph 0031).

As to claim 4, the combination of Dutcher and Chen et al. disclose the authentication apparatus according to claim 1. The combination fails to teach wherein said input unit inputs the authentication information using a web browser.

However, Foley discloses wherein said input unit inputs the authentication information using a web browser (Foley page 4, paragraph 0031).

It would be obvious to one of ordinary skill in the skill in the art at the time of the applicant's invention that web browsers were used to input authentication information into the system the user is trying to gain access to (Foley page 4, paragraph 0031).

As to claim 9, the combination of Dutcher and Chen et al. disclose the authentication method according to claim 7. The combination fails to teach wherein a card on which authentication information of an object of authentication has been recorded is read and said authentication information is input at said input step.

However, Foley discloses wherein a card on which authentication information of an object of authentication has been recorded is read and said authentication information is input at said input step (Foley page 4, paragraph 0031).

It would be obvious to one of ordinary skill in the skill in the art at the time of the applicant's invention that web browsers were used to input authentication information into the system the user is trying to gain access to (Foley page 4, paragraph 0031).

As to claim 10, the combination of Dutcher and Chen et al. disclose the authentication method according to claim 7. The combination fails to teach wherein the authentication information input by a web browser at said input step.

However, Foley discloses wherein the authentication information input by a web browser at said input step (Foley page 4, paragraph 0031).

It would be obvious to one of ordinary skill in the skill in the art at the time of the applicant's invention that web browsers were used to input authentication information into the system the user is trying to gain access to (Foley page 4, paragraph 0031).

As to claim 15, the combination of Dutcher and Chen et al. disclose the authentication method according to claim 13. The combination fails to teach wherein said first authentication step authenticates user-level access privilege, and said second authentication step manages administrator-level access privilege.

However, Foley discloses wherein said first authentication step authenticates user-level access privilege, and said second authentication step manages administrator-level access privilege (Foley page 3, paragraph 0026).

It would be obvious to one of ordinary skill in the skill in the art at the time of the applicant's invention that if both a user and a host can select a different level of authentication then the first step could be user-level and the second step could be administrator-level (Foley page 3, paragraph 0026).

As to claim 18, the combination of Dutcher and Chen et al. disclose the authentication apparatus according to claim 16. The combination fails to teach wherein said first authentication

unit authenticates user-level access privilege, and said second authentication unit manages administrator-level access privilege.

However, Foley discloses wherein said first authentication unit authenticates user-level access privilege, and said second authentication unit manages administrator-level access privilege (Foley page 3, paragraph 0026).

It would be obvious to one of ordinary skill in the skill in the art at the time of the applicant's invention that if both a user and a host can select a different level of authentication then the first step could be user-level and the second step could be administrator-level (Foley page 3, paragraph 0026).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ELENI A. SHIFERAW whose telephone number is (571)272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Eleni A Shiferaw/
Examiner, Art Unit 2436